

**This Page Is Inserted by IFW Operations
and is not a part of the Official Record**

BEST AVAILABLE IMAGES

**Defective images within this document are accurate representation of
The original documents submitted by the applicant.**

Defects in the images may include (but are not limited to):

- **BLACK BORDERS**
- **TEXT CUT OFF AT TOP, BOTTOM OR SIDES**
- **FADED TEXT**
- **ILLEGIBLE TEXT**
- **SKEWED/SLANTED IMAGES**
- **COLORED PHOTOS**
- **BLACK OR VERY BLACK AND WHITE DARK PHOTOS**
- **GRAY SCALE DOCUMENTS**

IMAGES ARE BEST AVAILABLE COPY.

**As rescanning documents *will not* correct images,
please do not report the images to the
Image Problem Mailbox.**

This Page Blank (uspto)



Europäisches
Patentamt

European
Patent Office

Office européen
des brevets

1c511 U.S. PTO
09/492632



Bescheinigung

Certificate

Attestation

Die angehefteten Unterla-
gen stimmen mit der
ursprünglich eingereichten
Fassung der auf dem näch-
sten Blatt bezeichneten
europäischen Patentanmel-
dung überein.

The attached documents
are exact copies of the
European patent application
described on the following
page, as originally filed.

Les documents fixés à
cette attestation sont
conformes à la version
initialement déposée de
la demande de brevet
européen spécifiée à la
page suivante.

Patentanmeldung Nr. Patent application No. Demande de brevet n°

99101913.4

Der Präsident des Europäischen Patentamts;
Im Auftrag

For the President of the European Patent Office

Le Président de l'Office européen des brevets
p.o.

LLC. Hatten-Heckman

DEN HAAG, DEN
THE HAGUE,
LA HAYE, LE

22/06/99

This Page Blank (uspto)



Europäisches
Patentamt

European
Patent Office

Office européen
des brevets

Blatt 2 der Bescheinigung
Sheet 2 of the certificate
Page 2 de l'attestation

Anmeldung Nr.:
Application no.:
Demande n°: 99101913.4

Anmeldetag:
Date of filing: 29/01/99
Date de dépôt:

Anmelder:
Applicant(s):
Demandeur(s):
International Business Machines Corporation
Armonk, NY 10504
UNITED STATES OF AMERICA

Bezeichnung der Erfindung:
Title of the invention:
Titre de l'invention:

Verbesserte digitale Signatur

Improved digital signature

In Anspruch genommene Priorität(en) / Priority(ies) claimed / Priorité(s) revendiquée(s)

Staat:
State:
Pays:

Tag:
Date:
Date:

Aktenzeichen:
File no.
Numéro de dépôt:

Internationale Patentklassifikation:
International Patent classification:
Classification internationale des brevets:

/

Am Anmeldetag benannte Vertragsstaaten:
Contracting states designated at date of filing: AT/BE/CH/CY/DE/DK/ES/FI/FR/GB/GR/IE/IT/LI/LU/MC/NL/PT/SE
Etats contractants désignés lors du dépôt:

Bemerkungen:
Remarks:
Remarques:

This Page Blank (uspto)

GE 999 005

- 1 -

B E S C H R E I B U N G**Verbesserte digitale Signatur**

Die Erfindung betrifft digitale Signaturen, Verfahren zum Erzeugen digitaler Signaturen und Signatureinrichtungen zur Durchführung der Verfahren.

Digitale Signaturen können als Gegenstück zur handgeschriebenen Signatur angesehen werden. Die von einem Absender unter einem elektronischen Dokument angebrachte digitale Signatur kann zur Feststellung der Identität des Absenders und der Authentizität des versendeten Dokuments verwendet werden. Die rechtliche Verbindlichkeit der digitalen Signatur ist ein wichtiges Thema für die öffentliche Verwaltung, für Unternehmen und in zunehmendem Maße auch für Privatpersonen.

Das Prinzip der digitalen Signatur ist bekannt. Es basiert auf einem asymmetrischen Verfahren, bei dem jeder Benutzer zwei verschiedene Schlüssel, einen geheimen (privaten) und einen öffentlichen, erhält, wobei der öffentliche Schlüssel allgemein zugänglich ist. Dabei setzt man voraus, daß jedes Schlüsselpaar einmalig ist. Mit dem privaten Schlüssel, der sich in der Regel auf einer Chipkarte befindet, wird die digitale Signatur durch den Absender erzeugt. Der Empfänger eines mit einer digitalen Signatur unterschriebenen Dokumentes kann unter Zuhilfenahme einer entsprechenden Software die Signatur vom Dokument trennen und mit Hilfe des öffentlichen Schlüssels des Absenders den Hash entschlüsseln und somit die Authentizität des Dokumentes und die Identität des Absenders überprüfen. Dieses Verfahren kann sowohl zwischen natürlichen Personen als auch zwischen Hardwareeinrichtungen verwendet werden.

Verfahren zur Erzeugung digitaler Unterschriften sind bekannt. So werden Signatureinrichtungen verwendet, die kryptographische Verfahren, wie z.B. das bekannte RSA (Rivest-Shamir-Adleman cryptographic algorithm)-Public-Key-Verfahren, nutzen. Dabei wird ein durch ein Hashing-Verfahren, wie z.B. MD5 (Message Digest #5) oder SHA-1 (Secure Hashing Algorithm) erzeugter Dokumentenauszugswert (Hash) mit dem privaten Schlüssel des Absenders signiert (verschlüsselt), und als digitale Signatur vor dem Versenden an das Dokument angefügt.

Bei kryptographischen Verfahren ist es notwendig, daß die Länge der digitalen Signatur mit der Länge des verwendeten Schlüssels, z.B. 512, 758 oder 1024 Bits, übereinstimmt. Da die Größe des Hash nur etwa 20 Byte beträgt, wird der ungenutzte Bereich der Signatur mit Füllzeichen (Pads) aufgefüllt. Somit werden bei einer digitalen Signatur beispielsweise 108 Bytes dieser Füllzeichen nutzlos gespeichert und transportiert, wenn ein 1024 Bit langer RSA-Schlüssel und der SHA-1 Hashing Algorithmus verwendet wird.

Bei den bekannten Verfahren erfolgt keine eindeutige Zuordnung der digitalen Signatur zu einer bestimmten Signatureinrichtung. Somit wäre es beispielsweise möglich, mit Hilfe eines gefälschten oder entwendeten Schlüssels und einer Signatureinrichtung ein Dokument mit einer gefälschten Signatur zu versehen. Der rechtmäßige Eigentümer des verwendeten Schlüssels hat dabei nur wenige oder keine Möglichkeiten nachzuweisen, ob eine solche nicht autorisierte Signatur tatsächlich ohne sein Wissen vorgenommen wurde.

Es wäre ebenfalls möglich, daß eine manipulierte oder entwendete Signiereinrichtung des Schlüsseleigentümers unter Verwendung eines Fremdprogrammes (Virus) dazu verwendet wird, ohne Wissen des Schlüsseleigentümers,

29-01-1999

EP99101913.4

SPEC

GE 999 005

- 3 -

Dokumente zu signieren. Dies könnte auch ohne Fremdeinwirkung geschehen, beispielsweise durch fehlerhafte Software oder Schnittstellen. Auch hier hat der Schlüsseleigentümer nur geringe Chancen die Unrechtmäßigkeit der dabei entstandenen Signaturen nachzuweisen.

Es ist daher Aufgabe der vorliegenden Erfindung, eine digitale Signatur bereitzustellen, mit deren Einsatz die rechtliche Verbindlichkeit einer digitalen Signatur erhöht wird.

Erfindungsgemäß wird diese Aufgabe durch die unabhängigen Ansprüche gelöst. Entsprechend der vorliegenden Erfindung wird eine erweiterte digitale Signatur geschaffen. Die erweiterte digitale Signatur umfaßt dabei neben dem Hash weitere Informationen. Dabei handelt es sich insbesondere um Informationen, welche die bei der Erzeugung der Signatur verwendete Hard- und Softwareumgebung kennzeichnet. Durch die erweiterte digitale Signatur wird die rechtliche Verbindlichkeit und damit auch die Anerkennung der digitalen Signatur wesentlich erhöht.

Die Erfindung ist nachstehend anhand von bevorzugten Ausführungsformen näher beschrieben. Es zeigt

- Fig.1 eine schematische Darstellung der Verwendung einer Chipkarte zum Erzeugen einer digitalen Signatur,
- Fig.2 eine schematische Darstellung einer Chipkarte zum Erzeugen einer digitalen Signatur entsprechend einem Ausführungsbeispiel,
- Fig.3 ein Ablaufdiagramm für das Verfahren zur Freigabe eines Signaturschlüssels,

- Fig.4 eine Darstellung eines Formulars zur Eingabe eines Signaturpaßwortes,
- Fig.5 ein Ablaufdiagramm für das Verfahren zur Erzeugung einer erweiterten digitalen Signatur nach der vorliegenden Erfindung,
- Fig.6 eine schematische Darstellung einer digitalen Signatur nach dem Stand der Technik,
- Fig.7 eine schematische Darstellung einer erweiterten digitalen Signatur nach der vorliegenden Erfindung.

In der bevorzugten Ausführungsform handelt es sich bei der Signatureinrichtung um Software auf einer Chipkarte. Eine solche Chipkarte 101 ist in Figur 1 dargestellt. Die Erfindung ist jedoch nicht auf Chipkarten beschränkt. Ebenso können andere Signatureinrichtungen, beispielsweise Kryptoadaptoren verwendet werden. Die Chipkarte wird hier zum Signieren eines Dokuments verwendet, welches beispielsweise auf einem Personalcomputer (PC) 102 erstellt wurde. Auf der Chipkarte befindet sich ein Chipkartenprogramm 106, welches hauptsächlich zum Signieren, also zur Verschlüsselung von Eingabedaten mit Hilfe eines privaten Schlüssels dient. Die Chipkarte 101 wird bei ihrer Auslieferung mit einer unveränderlichen und eindeutigen Seriennummer 103 versehen. Die Originalität der Seriennummer 103 kann mittels auf der Chipkarte gespeicherter kryptographischer Schlüssel überprüft werden, beispielsweise durch die bei Chipkarten üblichen Methoden 'external/internal authentication'.

Zum Versenden des Dokuments wird ein PC-Anwenderprogramm 104, beispielsweise Microsoft Outlook oder Netscape Navigator verwendet. Wie in Figur 1 gezeigt, dient ein

GE 999 005

- 5 -

spezielles Signaturprogramm 105, das auf dem PC 102 abläuft, als Schnittstelle zwischen der Chipkarte 101 mit dem Chipkartenprogramm zum Signieren 106 und dem PC-Anwenderprogramm 104.

Bevor die Chipkarte 101 zum Signieren verwendet werden kann, wird ein Signaturschlüssel 202, beispielsweise von einer Zertifizierungsstelle über den PC 102, auf die Chipkarte 101 übertragen. Dabei wird angenommen, daß der Eigentümer des Signaturschlüssels 202 gleichzeitig der Eigentümer der Chipkarte 101 ist. Das Übertragen des Signaturschlüssels 202 kann beispielsweise mit Hilfe des Signaturprogramms 105 geschehen. Der Signaturschlüssel 202 wird mit Hilfe des Chipkartenprogramms 106 auf der Chipkarte 101 als Bestandteil eines Zertifikats 201 gespeichert. Dies geschieht durch das Anlegen eines Schlüsselobjektes, beispielsweise durch einen Befehl 'create object' des Chipkartenprogramms 106. Weitere Bestandteile des Zertifikates 201 sind beispielsweise eine Bezeichnung des Zertifikates und eine Bezeichnung des verwendeten Verschlüsselungsverfahrens.

Durch den Einsatz bestehender Chipkartenbetriebssysteme für Chipkarten, beispielsweise dem in ISO 7816-4 beschriebenen, können Schlüsselobjekte, also auch Signaturschlüssel, sicher auf einer Chipkarte abgelegt werden. Der in dem Speicher der Chipkarte abgelegte Signaturschlüssel 202, beispielsweise ein 'Private Key' des RSA-Verfahrens, wird innerhalb des Chipkartenbetriebssystems beispielsweise mit den Zugriffsbedingungen 'Read=Never', 'Update=CHV1', 'Use=SignPW' geschützt (CHV1 - Card Holder Verification #1).

Zur weiteren Erhöhung der Sicherheit wird bei der Anlage des Schlüsselobjektes der Signaturschlüssel 202 zusammen mit einem 'secure sign'-Attribut 203 gespeichert, welches nach dem Anlegen des Signaturschlüssels 202 nicht mehr verändert

werden kann. Das 'secure sign' Attribut 203 unterscheidet spezielle Signaturschlüssel von anderen Schlüsselobjekten, die beispielsweise zur sonstigen Verschlüsselung von Daten verwendet werden. Alle anderen kryptographischen Verfahren der Chipkarte 101 können diesen speziellen Signaturschlüssel 202 nicht verwenden.

Bei dem Anlegen jedes Schlüsselobjektes mit dem 'secure sign'- Attribut 203 wird ein weiteres Attribut erzeugt, welches mit dem Signaturschlüssel 202 logisch verknüpft ist. Es entsteht ein Signaturschlüssel mit erweiterten Attributen. Bei diesem Attribut handelt es sich um einen Signaturzähler 204. Jedem Signaturschlüssel 202 ist also ein eigener Signaturzähler 204 zugeordnet.

Bei dem Signaturzähler 204 handelt es sich um einen einfachen digitalen Zähler. Um eine Manipulation zu erschweren, ist er im nichtflüchtigen Speicher auf der Chipkarte 101 untergebracht. In dem vorliegenden Beispiel hat der Signaturzähler 204 eine Größe von 4 Bytes (32 Bits Integer). Bei der Erzeugung des Signaturzählers 204 erhält er den Anfangswert 'Null'.

Die Größe des Signaturzählers 204 wird so gewählt, daß dieser bei normaler Lebensdauer der Chipkarte 101 nicht durch wiederholte Benutzung überläuft. Nach einem Überlauf (Wert aller Bits gleich 'Null') wird die Verwendung des Signaturschlüssels 202 intern gesperrt, um einen Betrug durch einen absichtlich herbeigeführten Überlauf zu verhindern. Der Signaturzähler 204 kann als Attribut des Signaturschlüssels 202 von der Chipkarte 101 ausgelesen, aber von außerhalb nicht verändert werden. Das kann beispielsweise durch das Chipkartenbetriebssystem mit der Zugriffsbedingung 'Read=never' sichergestellt werden.

GE 999 005

- 7 -

In der bevorzugten Ausführungsform wird die Sicherheit beim Erstellen einer digitalen Signatur nochmals erhöht, indem bei der Signierung eines Dokuments eine eindeutige Bestätigung jeder digitalen Signatur durch den Eigentümer des Signaturschlüssels 202 vorgesehen wird. Dies kann durch Eingabe eines Identifikationsmerkmals, beispielsweise eines Paßwortes oder einer PIN (Personal Identification Number), oder durch ein biometrisches Verfahren, beispielsweise das Einlesen eines Fingerabdruck geschehen. Handelt es sich bei dem Identifikationsmerkmal beispielsweise um ein Paßwort, so wird bei dem Anlegen jedes Schlüsselobjekts mit dem 'secure sign' Attribut neben dem Signaturzähler 204 noch ein weiteres Attribut, ein Signaturpaßwort 205, erzeugt, welches ebenfalls mit dem Signaturschlüssel 202 logisch verknüpft ist. Jedem Signaturschlüssel 202 ist also auch ein eigenes Signaturpaßwort 205 zugeordnet. Das Signaturpaßwort 205 wird bei seiner Erzeugung mit einem Anfangswert versehen, beispielsweise mit den Ziffern '123456'.

Durch die Verwendung des Signaturpaßwortes 205 wird ein unbeabsichtigtes Signieren von Dokumenten verhindert. Das Signaturpaßwort 205 zur Verwendung des Signaturschlüssels 202 existiert zusätzlich zu einem Paßwort zur Verwendung der Chipkarte 101. Damit wird eine Forderung des Gesetzes zur digitalen Signatur in Deutschland erfüllt, das vorsieht, daß pro durchzuführende Signatur das Paßwort abgefragt wird.

In der bevorzugten Ausführungsform der Erfindung muß vor der Erzeugung der ersten Signatur mit dem Signaturschlüssel 202 der Anfangswert des Signaturpaßworts 205 in ein individuelles Wert geändert werden. Dies dient der Erhöhung der Sicherheit. Nach der Ausgabe der Chipkarte 101 wird ein Signieren erst nach dieser Änderung möglich. In Figur 3 ist der Ablauf des Verfahrens zur initialen Freigabe des Signaturschlüssels 202 dargestellt. Nach Abschluß dieses

Verfahrens ist der Signaturschlüssel 202 zum digitalen Signieren freigegeben.

In Schritt 301 wird das Verfahren durch das Chipkartenprogramm zum Signieren 106 gestartet. Anschließend wird in Schritt 302 durch das Chipkartenprogramm überprüft, ob der Signaturschlüssel 202, beispielsweise wegen eines Überlaufs des Signaturzählers 204 oder einer defekten Hardware, gesperrt ist. Ist das der Fall, gibt das Chipkartenprogramm 106 in Schritt 303 eine Fehlermeldung an den Benutzer der Chipkarte 101 aus und beendet sich selbst.

Für den Fall, daß mehrere Signaturschlüssel 202 auf der Chipkarte 101 abgelegt sind, kann dem Benutzer der Chipkarte 101, beispielsweise durch das Chipkartenprogramm 106, vor Schritt 302 die Möglichkeit gegeben werden, festzulegen, welcher Signaturschlüssel 202 verwendet werden soll.

Ist der Signaturschlüssel 202 nicht gesperrt, wird der Benutzer der Chipkarte 101 in Schritt 304 aufgefordert, das Signaturpaßwort 205 einzugeben. Das eingegebene Signaturpaßwort 205 wird in Schritt 505 mit dem gültigen gespeicherten Signaturpaßwort verglichen.

Sind die verglichenen Signaturpaßwörter nicht identisch, wird in Schritt 306 ein Fehlbedienungszähler um den Wert 'Eins' erhöht. Der Fehlbedienungszähler dient zur Überwachung des Paßwortstatus und ist auf der Chipkarte 101 implementiert. Der Paßwortstatus kann beispielsweise durch die Zustände 'unverändert', 'verändert' und 'gesperrt' definiert sein. Die Verwendung des Signaturschlüssels 202 wird gesperrt, wenn die Anzahl der Fehlversuche eine vordefinierte Anzahl übersteigt (Paßwortstatus 'gesperrt').

Anschließend wird in Schritt 307 geprüft, ob der vorbestimmte Grenzwert des Fehlbedienungszählers erreicht

GE 999 005

- 9 -

ist. Ist das nicht der Fall, gibt das Chipkartenprogramm 106 in Schritt 308 eine Fehlermeldung aus und beendet sich selbst. Wurde der Grenzwert erreicht, sperrt das Chipkartenprogramm 106 in Schritt 309 den Signaturschlüssel 202 und beendet sich in Schritt 310 mit einer Fehlermeldung selbst.

Sind die in Schritt 305 verglichenen Signaturpaßwörter identisch, fordert das Chipkartenprogramm 106 den Benutzer der Chipkarte 101 in Schritt 311 auf, ein neues, individuelles Signaturpaßwort 205 einzugeben. Das eingegebene neue Signaturpaßwort 205 wird auf der Chipkarte 101 gespeichert und mit dem betreffenden Signaturschlüssel 202 logisch verknüpft.

Anschließend wird in Schritt 312 überprüft, ob der Signaturzähler 204 des Signaturschlüssels 202 den Anfangswert 'Null' hat. Ist das nicht der Fall, so wird das Verfahren in Schritt 313 abgebrochen, und ein Fehler in der Chipkarte 101 oder ein Mißbrauch des Signaturschlüssels 202 wahrscheinlich ist. Beträgt der Wert des Signaturzählers 204 'Null', so wird der Signaturzähler 204 in Schritt 314 auf den Wert 'Eins' erhöht und das Verfahren durch Schritt 315 beendet.

Der Wert des Signaturzählers 204 und der Paßwortstatus können in einer bevorzugten Ausführungsform, wie in Figur 4 dargestellt, dem Benutzer der Chipkarte 101 vor und/oder während der Paßwortänderung angezeigt werden. Ist der Signaturzähler 204 bei der Entgegennahme der Chipkarte 101 durch den Benutzer nicht auf dem Wert 'Null', und ist der Paßwortstatus nicht auf dem Originalzustand 'Unverändert', so ist das ein Indiz dafür, daß eine nicht vom Eigentümer der Chipkarte 101 autorisierte digitale Signatur vor der Auslieferung der Chipkarte erzeugt wurde.

Nachdem das Signaturpaßwort 205 erstmalig geändert worden ist, kann die Signierung eines Dokumentes stattfinden.

In Figur 5 ist der Ablauf des Signaturverfahrens unter Verwendung eines erweiterten Signaturschlüssels 202 dargestellt. Dabei besteht der erste Teil dieses Verfahrens aus den Schritten 501 bis 510, die mit den Schritten 301 bis 310 des in Figur 3 beschriebenen Verfahrens zur erstmaligen Freigabe des Signaturschlüssels 202 übereinstimmen, und in Figur 5 im einzelnen nicht wiederholt wiedergegeben wurden.

Sind die in Schritt 505 (entspricht Schritt 305 in Figur 3) verglichenen Paßwörter identisch, wird in Schritt 520 überprüft, ob der Signaturzähler 204 des Signaturschlüssels 202 den Anfangswert 'Null' hat. Ist das der Fall, wird der Signiervorgang in Schritt 521 mit der Ausgabe einer Fehlermeldung abgebrochen, da der Wert des Signaturzählers zur Erstellung einer Signatur wegen Schritt 314 aus Figur 3 nicht dem Anfangswert entsprechen darf.

Beträgt der Wert des Signaturzählers nicht 'Null', werden anschließend in Schritt 522 durch das Chipkartenprogramm 106 Informationen von außerhalb der Chipkarte angefordert. Bei diesen externen Informationen handelt es sich bevorzugt um Datum und Uhrzeit, beispielsweise im Format 'DDDDYYYYHHMMSS', die beispielsweise aus einer PC-Hardware oder PC-Software ausgelesen werden können. Eine weitere externe Informationen könnte die Identifikationsnummer des zu signierenden Dokuments sein, welche aus der PC-Software ausgelesen werden könnte, mit der das betreffende Dokument erzeugt wurde. Weiterhin könnte die Identifikationsnummer und/oder die Lizenznummer des verwendeten Signaturprogramms 105 als zusätzliche Information verwendet werden.

Das Chipkartenprogramm 106 liest anschließend in Schritt 523 die internen Informationen von der Chipkarte 101, also den

GE 999 005

- 11 -

Wert des Signaturzählers 204 des betreffenden Signaturschlüssels 202 und die Seriennummer 103 der Chipkarte 101 aus dem Speicher der Chipkarte 101. Eine weitere Information, die für eine erweiterte Signatur verwendet werden kann, ist eine Angabe darüber, welches kryptographische Verfahren, beispielsweise RSA, zur Erstellung der Signatur verwendet wird. Diese Information wurde zuvor bei der Erstellung des Signaturschlüssels 202 im Zertifikat 201 abgelegt. Eine weitere Information kann ein Identifikationsmerkmal des verwendeten Chipkartenprogramms zum Signieren 106 sein, beispielsweise die Lizenznummer oder Seriennummer des Programms.

Die externen und internen Informationen werden in Schritt 524 zusammen mit dem Hash auf der Chipkarte 101 zu einem Signaturdatensatz zu Erstellung der erweiterten digitalen Signatur zusammengefügt. Der Hash, der zuvor von dem PC-Anwenderprogramm 104 im PC 102 erzeugt wurde, ist dazu an das Chipkartenprogramm 106 gesendet worden. Das Zusammenfügen geschieht durch das Chipkartenprogramm. Dabei wird der Speicherplatz, der bisher nicht genutzt wurde und lediglich mit Füllzeichen belegt war, in einer definierten Reihenfolge mit den zusätzlichen externen und internen Informationen aufgefüllt. Eventuell verbleibenden freien Kapazitäten werden anschließend, wie in herkömmlichen Verfahren, mit Füllzeichen aufgefüllt. Im Hinblick auf die mögliche Verwendung der erweiterten Signatur als Standard ist eine verbindliche Definition der Reihenfolge als Standard notwendig.

Figur 6 zeigt eine schematische Darstellung einer herkömmlichen digitalen Signatur nach PKCS#1 (Public Key Cryptographic Standard). Im linken Teil befindet sich eine Kennzeichnung der Signatur (Block Typ). Im rechten Teil ist das vordefinierte Datenfeld zu erkennen, in dem der verschlüsselte Hash abgelegt ist. Dieser besitzt

üblicherweise eine Größe von etwa 20 Byte. Der Rest der Signatur wird, je nach Länge des verwendeten Signaturschlüssels 202, mit Füllzeichen im Umfang von 42, 74 oder 106 Bytes aufgefüllt.

Wie in Figur 5 dargestellt, wird im Anschluß an Schritt 524 der so entstandene Signaturdatensatz mit Hilfe des Signaturschlüssels 202 verschlüsselt. Es entsteht eine erweiterte digitale Signatur. Diese Verschlüsselung findet auf der Chipkarte 101 statt. Der aktuelle Wert des Signaturzählers 204, die Seriennummer 103 der Chipkarte 101 sowie die weiteren zusätzlichen Informationen als Teil des Signaturdatensatzes, werden, zusammen mit dem Hash, mit dem Signaturschlüssel 202 signiert.

In Figur 7 ist eine solche erweiterte digitale Signatur dargestellt. Dabei sind neben dem Hash auch der Wert des Signaturzählers 204 und die Seriennummer 103 der Chipkarte 101, sowie weitere interne und externe Informationen dargestellt, die als Signaturdaten eingefügt wurden. Bei den weiteren Informationen handelt es sich in diesem Beispiel im einzelnen um eine Identifikation (ID) des Chipkartenprogramms zum Signieren 106, Datum und Uhrzeit sowie um eine Identifikation des signierten Dokuments. Dabei ist die bevorzugte Größe der einzelnen Informationen in Byte angegeben. Das Format der resultierende Signatur ist mit dem aus dem bisherigen Verfahren kompatibel. Die bisher freie Kapazität der Füllzeichen wird für sinnvolle Informationen, mit deren Hilfe die verwendete Hardware- und Softwareumgebung eindeutig gekennzeichnet wird.

Durch Einbeziehung zusätzlicher Informationen in die digitale Signatur wird eine erweiterte digitale Signatur bereitgestellt, welche Rückschlüsse auf die Hard- und Softwareumgebung zuläßt, die bei der Signierung verwendet worden ist. Dabei sind insbesondere die beiden von der

GE 999 005

- 13 -

Chipkarte 101 stammenden Werte Signaturzähler 204 und Seriennummer 103 unverfälschlich.

Die Reihenfolge der mit einer bestimmten Chipkarte 101 vorgenommenen Signaturen ist somit durch den Absender verbindlich feststellbar. Auch hat der Empfänger von mehreren, mit einer erweiterten Signatur eines Absenders signierten Dokumenten die Möglichkeit festzustellen, in welcher Reihenfolge diese Dokumente signiert wurde. Das kann beispielsweise in solchen Fällen nützlich sein, wenn der Zeitpunkt des Unterzeichnens eines Dokuments eine ausschlaggebende Rolle spielt.

Nach der vorliegenden Erfindung kann der Eigentümer der Chipkarte 101 feststellen, ob seit der letzten (autorisierten) Erstellung einer digitalen Signatur mit der Chipkarte 101 weitere (nicht autorisierte) Signaturen mit seiner Chipkarte 101 erstellt wurden. Ebenso kann er die Anzahl dieser Signaturen feststellen. Ist der Signaturzähler 204 also gegenüber der letzten autorisierten Verwendung „n“ erhöht worden, so ist das ein Indiz dafür, daß nach der letzten Verwendung des betreffenden Signaturschlüssels 202 eine nicht vom Eigentümer der Chipkarte 101 autorisierte Erzeugung einer digitalen Signatur stattgefunden hat. Hilfreich zur Feststellung des Wertes des Signaturzählers 204 kann die Darstellung dieses Wertes für den Benutzer der Chipkarte 101 während des Signierens sein. Für die nachträglichen Feststellung des Wertes des Signaturzählers 204 in der Signatur eines zuvor versendeten Dokumentes ist die Speicherung aller mit einer digitalen Signatur versehenen Dokumente sinnvoll.

Bei Verlust der Chipkarte 101 und Wiederauffinden kann durch Überprüfen des Signaturzählers 204 und durch den Vergleich mit dem Zählerwert der letzten autorisierten Signatur leicht festgestellt werden, ob der Signaturschlüssel 202

mißbräuchlich verwendet wurde. Die digitalen Signaturen mit den Zählerwerten ,n+1' bis ,m-1', wobei m der aktuellen Zählerstand ist, wurden demnach nichtautorisiert vorgenommen. Die mißbräuchlich signierten Dokumente können an Hand des Zählerstandes des Signaturzählers 204 eindeutig identifiziert und zurückgewiesen werden.

Ebenso ist die eindeutige Zuordenbarkeit einer Signatur zu einer bestimmten Chipkarte 101 gewährleistet. Der Benutzer einer Chipkarte 101 kann daher feststellen, ob eine bestimmte Signatur tatsächlich mit seiner Chipkarte erzeugt wurde.

Da die Struktur der digitalen Signatur festgelegt ist, ist es auf Empfängerseite einfach möglich, die entsprechenden zusätzlichen Informationen zu isolieren und auszuwerten. Dazu könnte eine angepaßte Software auf dem PC des Empfängers dienen.

Wie in Schritt 526 in Figur 5 dargestellt, wird der Signaturzähler 204 des verwendeten Signaturschlüssels 202 nach jeder Erzeugung einer digitalen Signatur um den Wert ,Eins' erhöht. Damit wird eine Durchnummerierung der erzeugten digitalen Signaturen entsprechend ihrer zeitlichen Abfolge vorgenommen.

Die erweiterte digitale Signatur wird in Schritt 527 an das Signaturprogramm 105 übergeben. Damit endet die Erzeugung der erweiterten digitalen Signatur in Schritt 528.

Die so erzeugte digitale Signatur kann jetzt an das zu versendende Dokument angefügt werden. Das kann derart erfolgen, daß die erweiterte Signatur von dem Signaturprogramm 105 an das PC-Anwenderprogramm 104 übergeben wird, und dort mit dem zu versendenden Dokument verbunden wird.

GE 999 005

- 15 -

Bevorzugt wird wiederum, beispielsweise wie auch in Figur 4 dargestellt, vor und/oder während des Signierens der Wert des Signaturzählers 204 und der Paßwortstatus dem Benutzer der Chipkarte 101 angezeigt. Zur weiteren Erhöhung der Sicherheit und zur besseren Kontrolle kann auch die Seriennummer 103 der Chipkarte 101 während des Signierens angezeigt werden. Dies ermöglicht es dem Benutzer der Chipkarte 101, den einwandfreien Zustand der Chipkarte zu überprüfen.

P A T E N T A N S P R Ü C H E

1. Verfahren zur Erzeugung einer digitalen Signatur in einer Signatureinrichtung (101) für die Signierung eines Dokuments, mit den Schritten:
 - a) Beschaffen von Informationen,
 - b) Erzeugung eines Signaturdatensatzes, der mindestens die in Schritt a) beschafften Informationen und einen Dokumentenauszugswert des zu signierenden Dokuments umfaßt,
 - c) Erzeugen einer erweiterten digitalen Signatur durch Verschlüsseln des Signaturdatensatzes mit Hilfe eines Signaturschlüssels (202).
2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß Schritt a) die Beschaffung des Wertes eines Signaturzählers (204) umfaßt.
3. Verfahren nach Anspruch 2, dadurch gekennzeichnet, daß der Signaturzähler (204) zuvor als Attribut des Signaturschlüssels (202) erstellt wurde.
4. Verfahren nach einem der Ansprüche 1 bis 3, dadurch gekennzeichnet, daß Schritt a) die Beschaffung eines Identifikationsmerkmals (103) zur Identifizierung der Signatureinrichtung umfaßt.
5. Verfahren nach einem der Ansprüche 1 bis 4, dadurch gekennzeichnet, daß Schritt a) die Beschaffung von Angaben über die Hard- und Softwareumgebung bei der Erzeugung der digitalen Signatur umfaßt.

GE 999 005

- 17 -

6. Verfahren nach einem der Ansprüche 1 bis 5, dadurch gekennzeichnet, daß vor Schritt a) die Eingabe eines Identifikationsmerkmals (205) zur Identifizierung des Eigentümers des Signaturschlüssels (202) erfolgt.
7. Verfahren nach Anspruch 6, dadurch gekennzeichnet, daß das Identifikationsmerkmal (205) zur Identifizierung des Eigentümers des Signaturschlüssels (202) zuvor als Attribut des Signaturschlüssels (202) erstellt wurde.
8. Verfahren nach Anspruch 6 oder 7, dadurch gekennzeichnet, daß vor dem erstmaligen Durchlaufen des Schrittes a) eine Änderung des Identifikationsmerkmal (205) zur Identifizierung des Eigentümers des Signaturschlüssels (202) erfolgt.
9. Signatureinrichtung (101), dadurch gekennzeichnet, daß sie eine Vorrichtung (106) zur Durchführung des Verfahrens nach einem der Ansprüche 1 bis 8 umfaßt.
10. Signatureinrichtung (101) nach Anspruch 9, dadurch gekennzeichnet, daß es sich um eine Chipkarte handelt.
11. Digitale Signatur, dadurch gekennzeichnet, daß sie neben einem Dokumentenauszugswert eines zu signierenden Dokuments weitere Informationen enthält.
12. Digitale Signatur nach Anspruch 11, dadurch gekennzeichnet, daß sie Informationen umfaßt, die sie gegenüber jeder anderen digitalen Signatur, die mit dem gleichen Signaturschlüssel (202) erzeugt worden ist, eindeutig kennzeichnet.
13. Digitale Signatur nach Anspruch 11 oder 12, dadurch gekennzeichnet, daß sie Informationen darüber umfaßt,

mit welcher Signatureinrichtung (101) die digitale Signatur vorgenommen wurde.

14. Digitale Signatur nach einem der Ansprüche 11 bis 13, dadurch gekennzeichnet, daß sie Informationen über die Hard- und Softwareumgebung bei der Erzeugung der digitalen Signatur umfaßt.

1 / 4

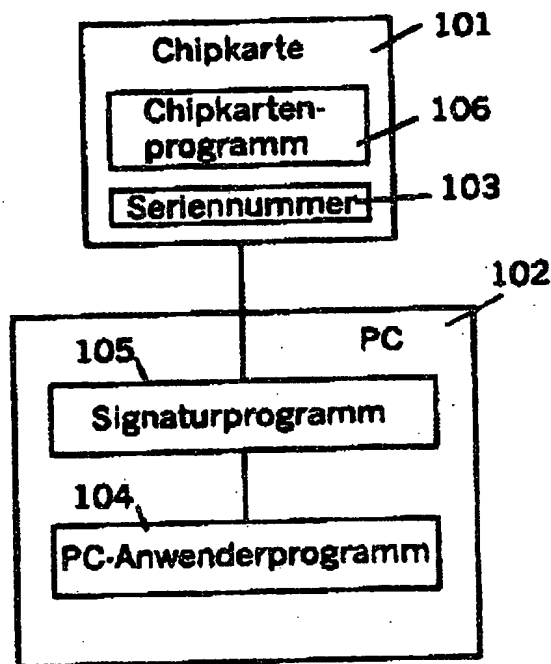


FIG. 1

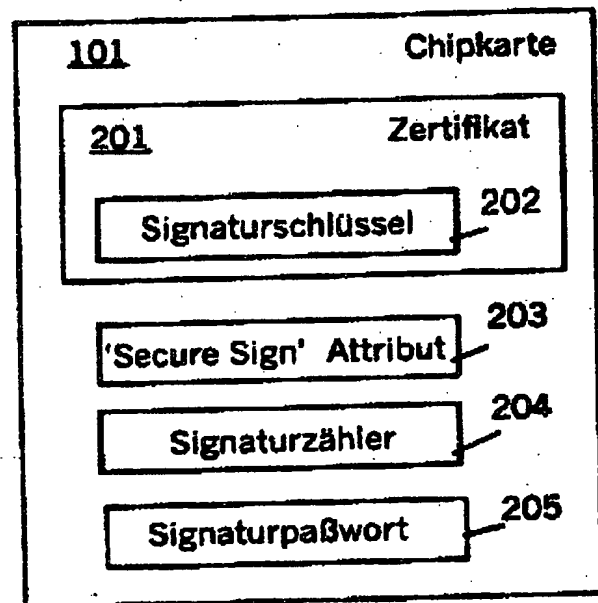


FIG. 2

Diagram illustrating a user interface for signing. The window displays the following elements:

- Nummer der Signatur: 4
- Paßwortstatus: unverändert
- Bitte Signaturpaßwort eingeben:
- Input field for the password (displayed as * * * *)
- Buttons: Signieren, Abbruch

FIG. 4

2 / 4

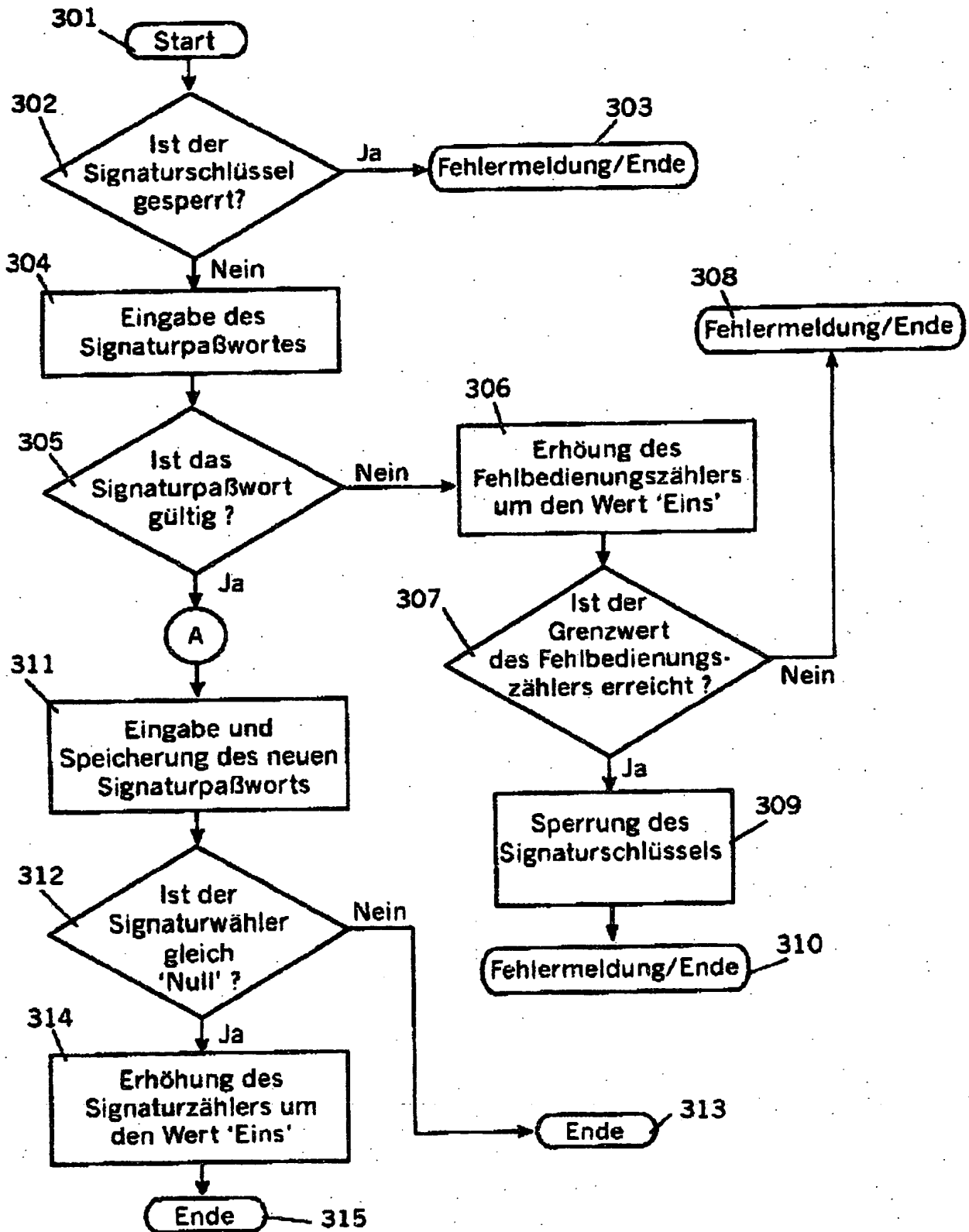


FIG. 3

3 / 4

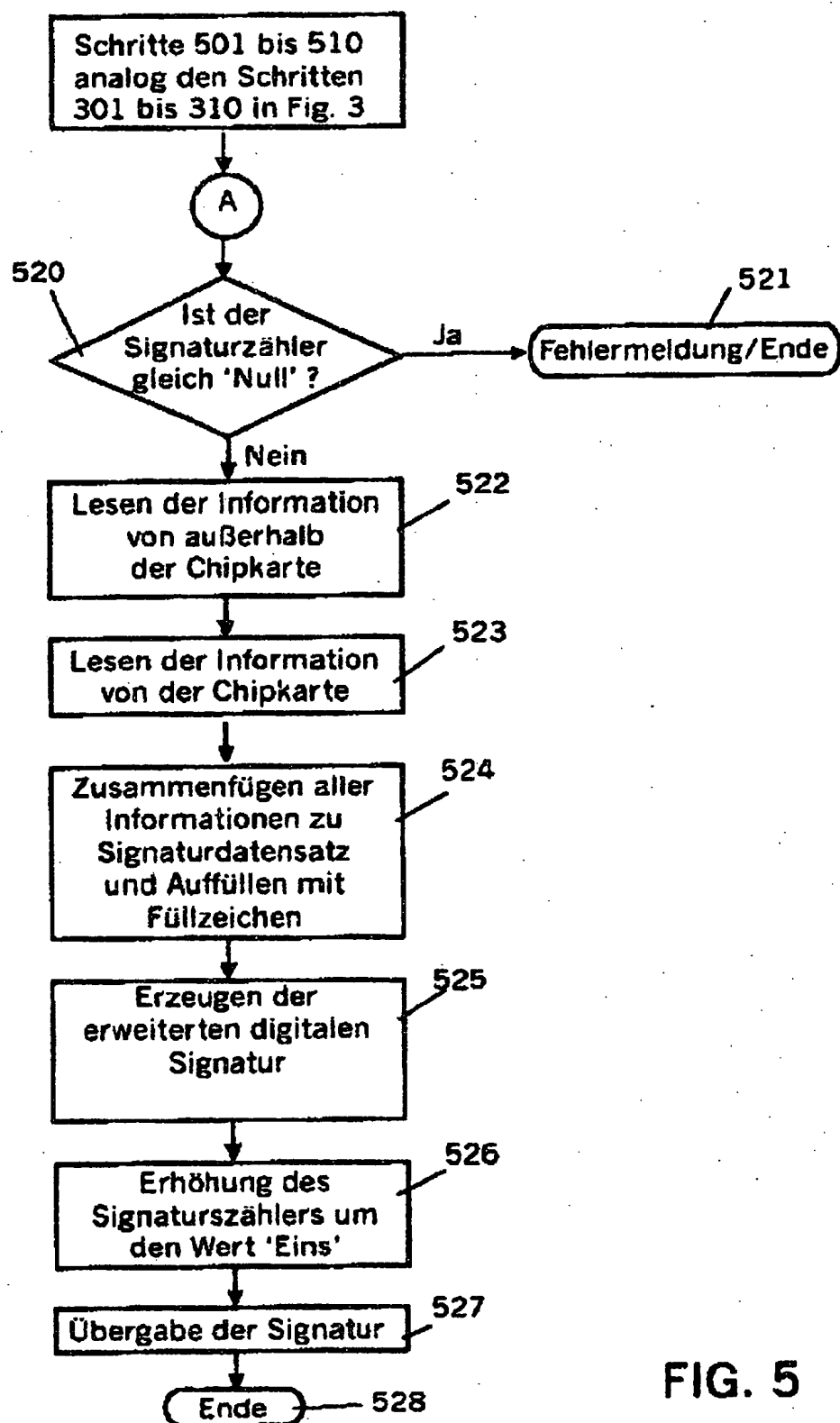


FIG. 5

Block Typ	Füllzeichen	Hash
2	42/74/106	20

FIG. 6

Block Typ	Füll- zeichen	Dokument ID	Datum & Uhrzeit	Chipkarten- programm ID	Chipkarten- serien- nummer	Signatur- zähler	Hash
2			7	16	16	4	20

FIG. 7

GE 999 005

- 19 - ;

Z U S A M M E N F A S S U N G

Die Erfindung betrifft die Erzeugung digitaler Signaturen, mit deren Einsatz die rechtliche Verbindlichkeit von digitalen Signaturen erhöht wird. Dazu wird eine erweiterte digitale Signatur geschaffen, die neben dem Hash zusätzliche Informationen umfaßt. Dabei handelt es sich insbesondere um Informationen, welche die bei der Erzeugung der Signatur verwendete Hard- und Softwareumgebung kennzeichnet.

This Page Blank (uspto)